

## 2 Factor Authentication

### What does Multi-Factor Authentication mean for me?

So, you have gotten an email from someone in IT or perhaps even your boss saying that they have added additional security verification to your account. So what does this mean?

Not to worry. That simply means that your organization wants to take some extra steps to ensure that you are who you say you are when signing in to your Office 365 apps such as email, one drive and anything else in office 365. This is done by using a combination of your user name and password and a phone. Either your office phone or a smart phone. Two-step verification is an additional security step that helps protect your account by making it harder for other people to access your account.

So the first thing you are going to need to do is complete the enrollment process. But before we start that process there are a few things to decide.

- **Office phone or mobile phone** - Choose between using your office phone or your mobile phone.
- **Office phone call** –If using a desk/office phone, need to be by the phone when accessing your email, you will receive a call.
- **Mobile phone call, text or mobile app** - If using a mobile phone, choose between receiving a call, a text, or using the mobile app.
- **Mobile app with a notification or verification code** - If using the mobile app, choose between receiving a notification that you respond to or a verification code.
- **App Passwords**- If you are using the native apple email program on your desktop and/or native apple email on your iphone, ipad, and/or native android mail app on your android phone or tablet, you will need to setup **App Passwords** through your RWU o365 portal account.

**For more info, please click on following link:**

<https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-end-user/>

<https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-end-user-app-passwords/>

## Set up my account for two-step verification

Two-step verification is an additional security step that helps protect your account by making it harder for other people to break in. If you're reading this article, you probably got an email from your work or school admin about Multi-Factor Authentication. Or maybe you tried to sign in and got a message asking you to set up additional security verification. If that's the case, **you cannot sign in until you have completed the auto-enrollment process.**

## Use a mobile app as the contact method

Using this method requires that you install an authenticator app on your phone or tablet. The steps in this article are based on the Microsoft Authenticator app, which is available for [Windows Phone](#), [Android](#), and [IOS](#).

1. Select **Mobile app** from the drop-down list.
2. Select either **Receive notifications for verification** or **Use verification code**, then select **Set up**.

Microsoft Azure

### Additional security verification

Secure your account by adding phone verification to your password. [View video](#)

**Step 1: How should we contact you?**

Mobile app

Method

Notification

One-time password

To use these verification methods, you must set up the Multi-Factor Authentication app.

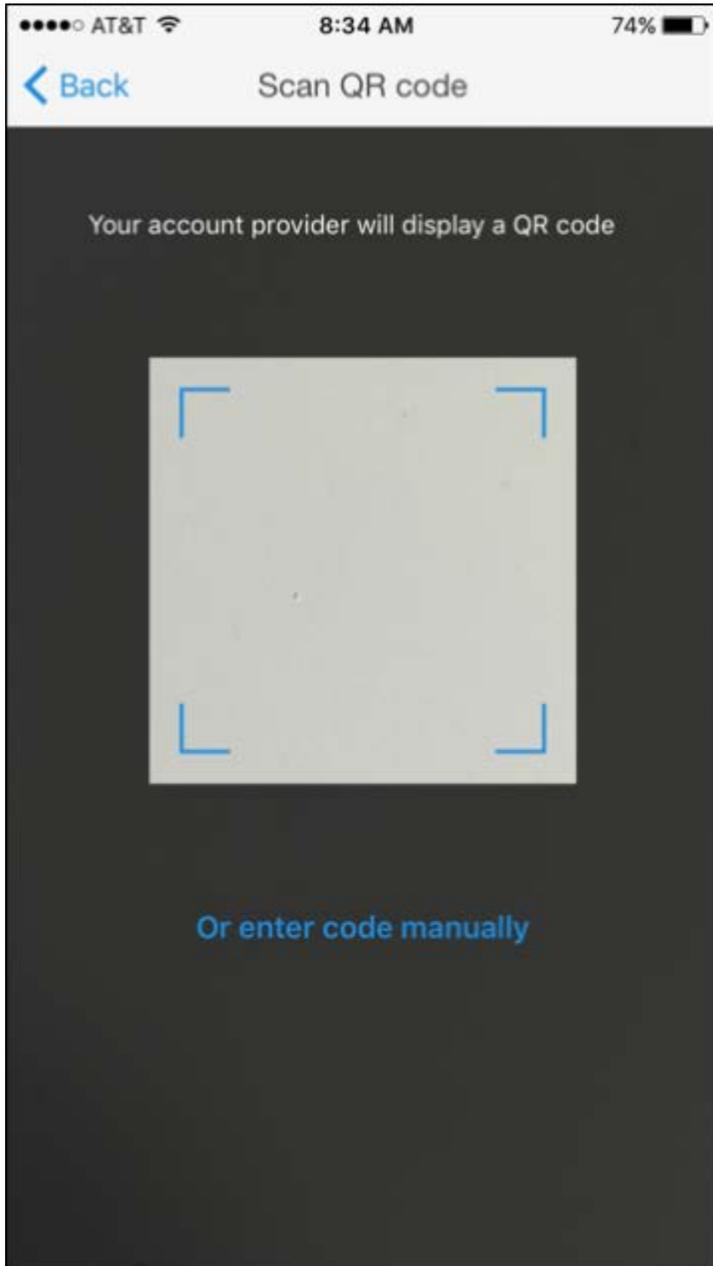
**Set up** Please configure the mobile app.

Contact me

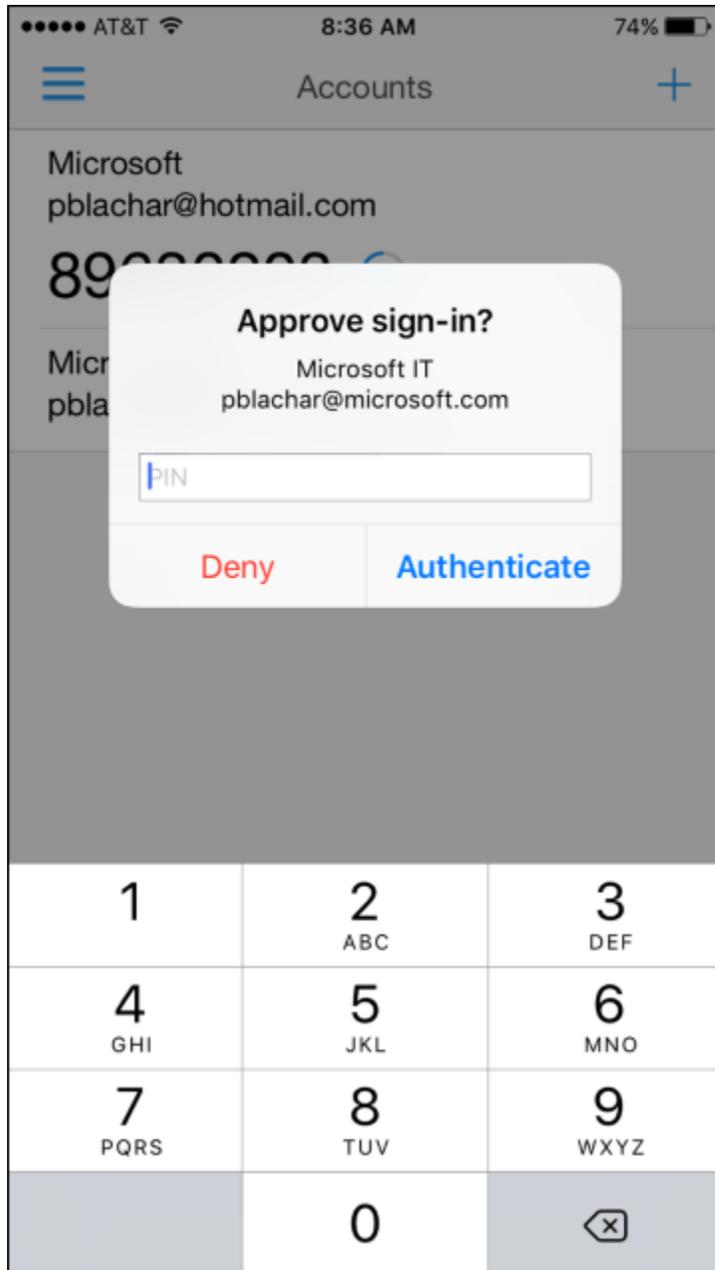
©2015 Microsoft Legal | Privacy

3. On your phone or tablet, open the app and select + to add an account. (On Android devices, select the three dots, then **Add account**.)

- Specify that you want to add a work or school account. The QR code scanner on your phone opens. If your camera is not working properly, you can select to enter your company information manually. For more information, see [Add an account manually](#).
- Scan the QR code picture that appeared with the screen for configuring the mobile app. Select **Done** to close the QR code screen.



- When activation finishes on the phone, select **Contact me**. This step sends either a notification or a verification code to your phone. Select **Verify**.
- If your company requires a PIN for approving sign-in verification, enter it.



8. After PIN entry is complete, select **Close**. At this point, your verification should be successful.
9. We recommend that you enter your mobile phone number in case you lose access to your mobile app. Specify your country from the drop-down list, and enter your mobile phone number in the box next to the country name. Select **Next**.
10. At this point, you are prompted to set up app passwords for non-browser apps such as Outlook 2010 or older, or the native email app on Apple devices. This is because some apps don't support two-step verification. If you do not use these apps, click **Done** and skip the rest of the steps.
11. If you are using these apps, copy the app password provided and paste it into your application instead of your regular password. You can use the same app password for multiple apps. For more info, [help with app passwords].

12. Click **Done**.

Add an account manually

If you want to add an account to the mobile app manually, instead of using the QR reader, follow these steps.

1. Select the **Enter account manually** button.
2. Enter the code and the URL that are provided on the same page that shows you the barcode. This info goes in the **Code** and **URL** boxes on the mobile app.

### Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Multi-Factor Authentication app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, tap '+' to add a user.
3. Tap the 'Scan Barcode' icon. This will launch the camera.
4. Scan the image below.



If you are unable to scan the image, enter the following information in your app.

CODE: 056 064 843

URL: <https://bn1pfpad12.phonefactor.net/pad/356051542>

If the app displays a six-digit code, you are done!

Done [cancel](#)

3. When the activation has finished, select **Contact me**. This step sends either a notification or a verification code to your phone. Select **Verify**.

# Use your mobile phone as the contact method

1. Select **Authentication Phone** from the drop-down list.

Microsoft Azure

## Additional security verification

Secure your account by adding phone verification to your password. [View video](#)

**Step 1: How should we contact you?**

Authentication phone ▼

United States (+1) ▼

Method

Send me a code by text message

Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2015 Microsoft Legal | Privacy

2. Choose your country from the drop-down list, and enter your mobile phone number.
3. Select the method you would prefer to use with your mobile phone - text or call.
4. Select **Contact me** to verify your phone number. Depending on the mode you selected, we send you a text or call you. Follow the instructions provided on the screen, then select **Verify**.
5. At this point, you are prompted to set up app passwords for non-browser apps such as Outlook 2010 or older, or the native email app on Apple devices. This is because some apps don't support two-step verification. If you do not use these apps, click **Done** and skip the rest of the steps.
6. If you are using these apps, copy the app password provided and paste it into your application instead of your regular password. You can use the same app password for multiple apps. For more info, [help with app passwords].
7. Click **Done**.

# Use your office phone as the contact method

1. Select **Office Phone** from the drop-down

Microsoft Azure

## Additional security verification

Secure your account by adding phone verification to your password. [View video](#)

**Step 1: How should we contact you?**

Office phone ▼

Select your country or region ▼ Extension

Contact your admin if you need to update your office number. Do not use a Lync phone.

Contact me

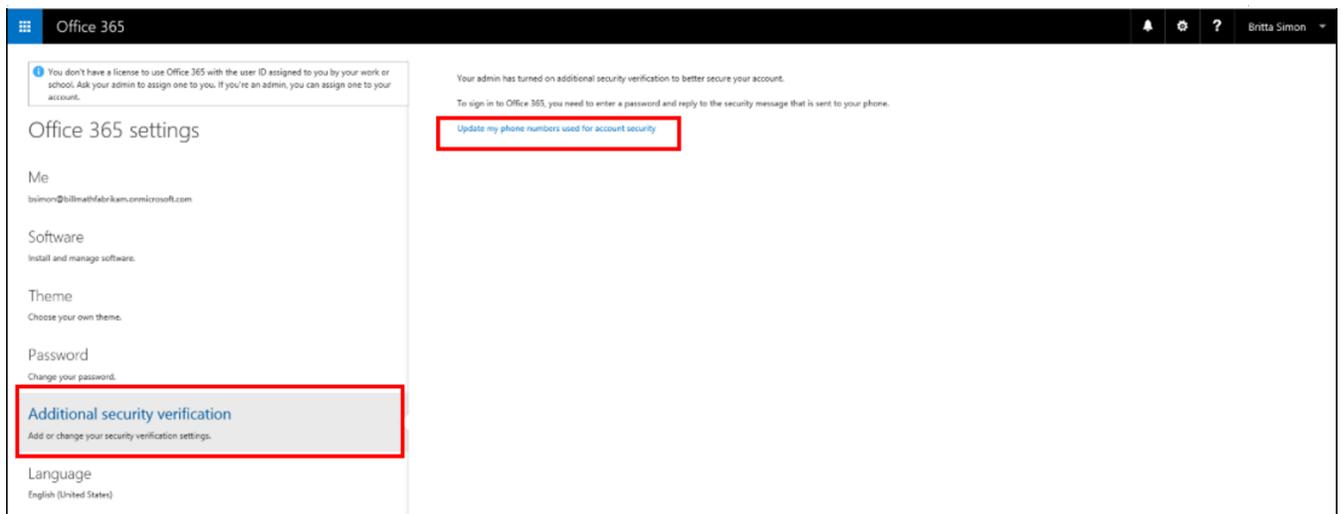
Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2015 Microsoft Legal | Privacy

2. The phone number box is automatically filled with your company contact information. If the number is wrong or missing, ask your admin to make changes.
3. Select **Contact me** to verify your phone number, and we will call your number. Follow the instructions provided on the screen, then select **Verify**.
4. At this point, you are prompted to set up app passwords for non-browser apps such as Outlook 2010 or older, or the native email app on Apple devices. This is because some apps don't support two-step verification. If you do not use these apps, click **Done** and skip the rest of the steps.
5. If you are using these apps, copy the app password provided and paste it into your application instead of your regular password. You can use the same app password for multiple apps. For more info, see [What are App Passwords](#).
6. Click **Done**.

# Creating app passwords

1. Log on to the [Office 365 portal](#).
2. In the top right corner select the widget and choose Office 365 Settings.
3. Click on Additional security verification.
4. On the right, click the link that says **Update my phone numbers used for account security**.



- This will take you to the page that will allow you to change your settings.

The screenshot shows the 'Additional security verification' page for app passwords in Office 365. The page title is 'Additional security verification app passwords'. Below the title, there is a brief explanation: 'When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.' A 'View video' link is provided. The page asks 'what's your preferred option?' and 'how would you like to respond?'. There are three main options for responding: 'Authentication phone', 'Office phone', and 'Alternate authentication phone'. Each option has a dropdown menu for 'Select your country or region' and a text input for the phone number. The 'Authentication phone' option is selected, and the country is set to 'United States (+1)'. The 'Azure Authenticator app' option is also selected, and a 'Configure' button is visible next to it. At the bottom, there are 'Save' and 'cancel' buttons. A note at the bottom states: 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.'

- At the top, next to additional security verification, click on **app passwords**.

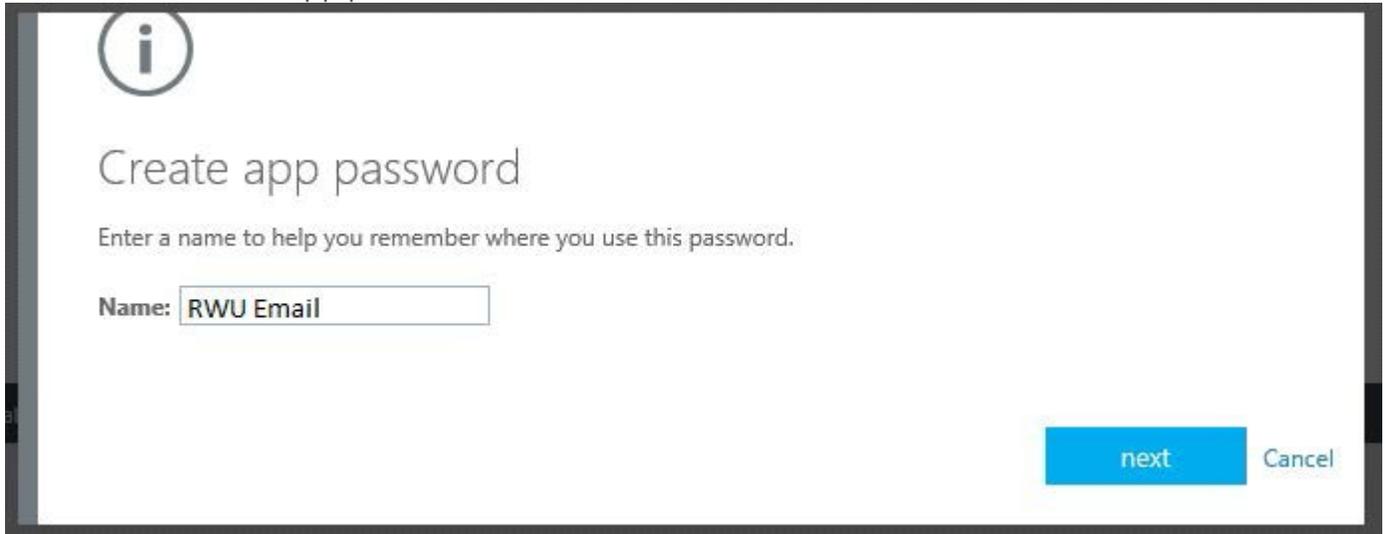
- Click **Create**.

The screenshot shows the 'app passwords' page in Office 365. The page title is 'additional security verification app passwords'. Below the title, there is an explanation: 'To sign into Outlook, Lync or other apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.' A 'Learn more' link is provided. The page also states: 'You can use the same app password with multiple apps or create a new app password for each app. How do I get my apps working with app passwords?'. A note follows: 'Note: If you are an admin of a Microsoft service, we recommend not using app passwords.' A 'Bookmark this page' link is also present. A 'create' button is visible. Below the button, there is a table with two columns: 'NAME' and 'DATE CREATED'. The table contains one row with the following data:

NAME	DATE CREATED
Initial app password20150320175734	3/20/2015

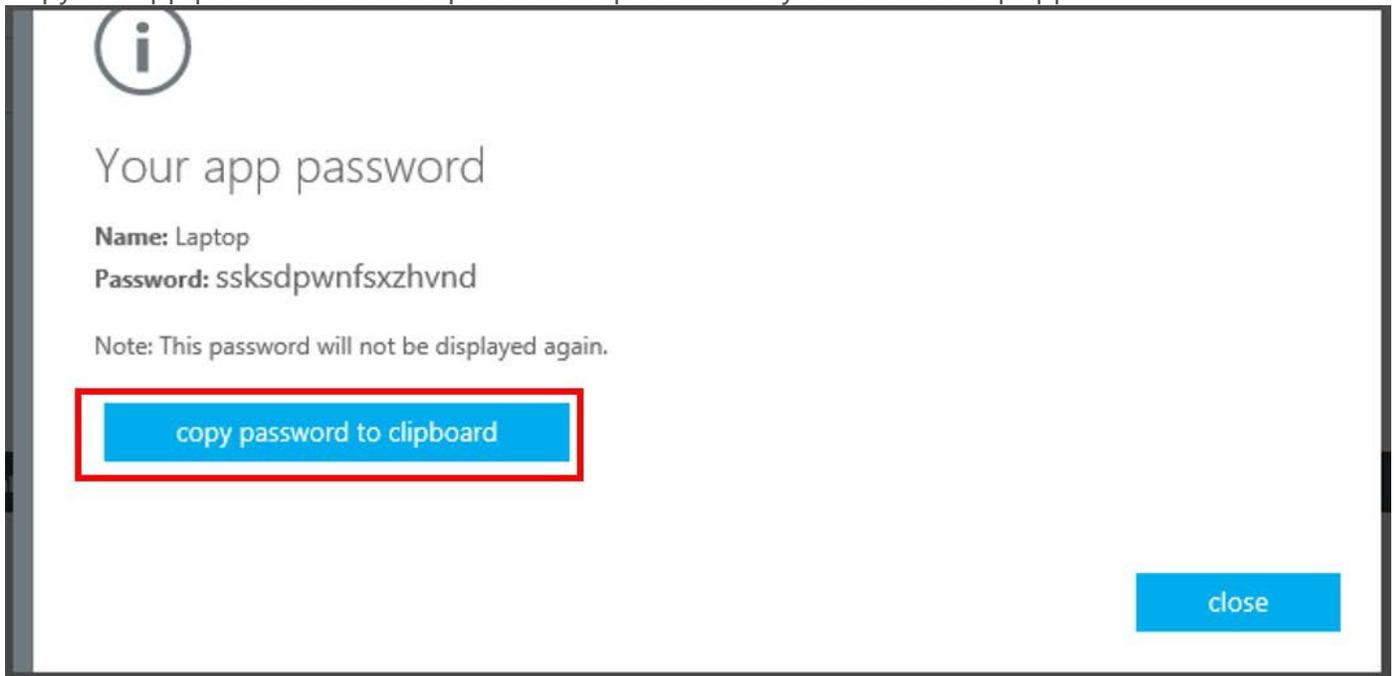
A 'Delete' link is visible next to the row in the table.

8. Enter a name for the app password and click **Next**.



The screenshot shows a dialog box titled "Create app password". At the top left is an information icon (a lowercase 'i' in a circle). Below the title, there is a subtitle: "Enter a name to help you remember where you use this password." Below this is a text input field with the label "Name:" and the text "RWU Email" entered. In the bottom right corner, there are two buttons: a blue button labeled "next" and a grey button labeled "Cancel".

9. Copy the app password to the clipboard and paste it into your email desktop app.



The screenshot shows a dialog box titled "Your app password". At the top left is an information icon (a lowercase 'i' in a circle). Below the title, there is a subtitle: "Your app password". Below this, there are two lines of text: "Name: Laptop" and "Password: ssksdpwnfsxzhvnd". Below the password is a note: "Note: This password will not be displayed again." In the bottom left corner, there is a blue button labeled "copy password to clipboard" which is highlighted with a red rectangular border. In the bottom right corner, there is a blue button labeled "close".